UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,291	12/03/2003	Brian C. Morris	S-00014-011	6923

25179   7590   05/12/2008
A PATENT LAWYER CORP, PLC
R WILLIAM GRAHAM
22 S ST CLAIR ST
DAYTON, OH 45402

EXAMINER
WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
05/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 April 2008*.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-19* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

1   **DETAILED ACTION**

2

3   Claims 1 – 19 are pending.

4   This action is in response to the communication filed on 4/1/08.

5   All objections and rejections not set forth below have been withdrawn.

6

7   *Continued Examination Under 37 CFR 1.114*

8

9   A request for continued examination under 37 CFR 1.114, including the fee set

10   forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this

11   application is eligible for continued examination under 37 CFR 1.114, and the fee set

12   forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action

13   has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/1/08

14   has been entered.

15

16

17   *Claim Rejections - 35 USC § 103*

18

19   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

20   obviousness rejections set forth in this Office action:

21   (a) A patent may not be obtained though the invention is not identically disclosed or described as set
22   forth in section 102 of this title, if the differences between the subject matter sought to be patented and
23   the prior art are such that the subject matter as a whole would have been obvious at the time the
24   invention was made to a person having ordinary skill in the art to which said subject matter pertains.
25   Patentability shall not be negatived by the manner in which the invention was made.

1

2   **Claims 1 – 8 and 10 – 18 are rejected under 35 U.S.C. 103(a) as being**

3   **unpatentable over Aziz et al. (Aziz), "Method and Apparatus for Providing Secure**

4   **Communication with a Relay in a Network", U.S. Patent 6,643,701 in view of Gast,**

5   **"System and Method for Accelerating Cryptographically Secured Transactions",**

6   **U.S. Patent Publication 2003/0046532.**

7

8   Regarding claim 1, Aziz discloses a system for establishing first (fig. 3:310) and

9   second SSL connections (fig. 3:330) between a client and a web server. The system

10 comprises:

11   *a web server computer having SSL protocol server software operably associated*

12 *therewith for enabling a SSL connection, wherein SSL protocol server software includes*

13 *a CA certificate and private key* (fig. 3:340; 6:21-24),

14   *and a client computer communicatively linked to said web server computer*

15 *having web browser software having SSL protocol client software operably associated*

16 *therewith for enabling an a first SSL connection between said client computer and said*

17 *web server computer* (fig. 3:300; 6:18-21),

18   Aziz discloses client and server software operably associated with the client

19 computer and the web server computer (fig. 3:320; 6:4-26). Aziz does not appear to

20 explicitly recite that such software is "SSL acceleration software". However, Gast

21 explicitly recites that client and server software can be for the purpose of acceleration

22 (Abstract, fig. 2:200). It would have been obvious to one of ordinary skill in the art to

23 recognize the benefits of acceleration as disclosed by Gast within the system of Aziz.

1   This would have been obvious because one of ordinary skill in the art would have been

2   motivated by the advantages of speed and efficiency.

3   The combination enables:

4   SSL acceleration server software *operably associated with said web server*

5   *computer which includes a pseudo CA certificate and access to said private key and a*

6   *public key* (Aziz, fig. 3:320; 5:6-13; Gast, fig. 2:202,214, 206, 212) and *SSL acceleration*

7   *client software operably associated with said client computer* (Aziz, fig. 3:320; 5:6-13;

8   Gast, fig. 2:202,214, 206, 212) *which communicates with said SSL acceleration server*

9   *software to receive a copy of said pseudo CA certificate and said public key and present*

10   *said pseudo CA certificate to said web browser software for validation thereof for*

11   *enabling a second SSL connection between said client computer and said web server*

12   *computer in a manner which permits optimization techniques to be applied on data*

13   *transmitted through said second SSL connection* (Gast, fig. 2:202, 214, 206, 212).

14

15   Regarding claim 2, the combination enables:

16   *wherein said SSL acceleration client software is further equipped for monitoring*

17   *when said web browser requests a SSL connection with said web server computer and*

18   *intercepting said SSL request from said web browser, and diverting communication*

19   *through one of an established and an initiated SSL connection through said SSL*

20   *acceleration client software and SSL acceleration server software* (Aziz, 4:49-65; 7:54-

21   8:5).

22

1   Regarding claim 3, the combination enables:

2   *wherein said SSL acceleration client software is equipped to initiate a SSL*

3   *request to said SSL acceleration server software operably disposed with web server*

4   *computer to establish a SSL connection* (Aziz, 4:49-65; 7:54-8:5; Gast, fig. 2:202, 206,

5   212).

6

7   Regarding claim 4, the combination enables:

8   *wherein SSL acceleration server software is further equipped for monitoring*

9   *when the web server computer receives a request for a SSL connection through said*

10 *SSL acceleration client software where upon such request initiates a SSL handshake*

11 *wherein said pseudo CA certificate is sent to said client computer via SSL acceleration*

12 *client software with a public key* (Aziz, 5:1-22).

13

14   Regarding claim 5, the combination enables:

15   *wherein said web browser software is equipped to send a list of available*

16 *encryption algorithms to said web server computer and said SSL acceleration client*

17 *software intercepts said list, selects an encryption algorithm from said list* (Aziz, 1:33-63;

18 Gast, par. 24-26).

19

20   Regarding claim 6, the combination enables:

1   *wherein said SSL acceleration client software is equipped to send said chosen*

2   *encryption algorithm to said browser software* (Gast, par. 24 – herein the combination

3   discloses that the data is relayed from one end system to the other).

4

5   Regarding claim 7, the combination enables:

6   *wherein said browser software is equipped to create a secret key, encrypt using*

7   *said chosen encryption algorithm and using said public key and send said encrypted*

8   *secret key to said server computer through said SSL acceleration client software/SSL*

9   *acceleration server software* (Aziz, 2:1-36).

10

11   Regarding claim 8, the combination enables:

12   wherein said SSL acceleration server software is equipped to de-encrypt said

13   secret key using said private key (Aziz, 2:1-36; 5:1-22).

14

15   Regarding claims 10 – 18, they comprise essentially similar limitations to the

16   rejected claims above, and they are rejected, at least, for the same reasons.

17

18   **Claims 9 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable**

19   **over the combination of Aziz and Gast in view of Freed et al. (Freed), "Secure**

20   **Sockets Layer Proxy Architecture", U.S. Patent Publication 2003/0014628.**

21

1   Regarding claims 9 and 19, the combination recites software for transforming

2   SSL data transmissions, but does not appear to explicitly recite compression. Freed,

3   however, teaches that SSL data transmissions are transformed by compression (Freed,

4   par. 10, 52). It would have been obvious to one of ordinary skill in the art to employ

5   compression within the SSL data transmission of the combination of Aziz and Gast.

6   This would have been obvious because one of ordinary skill in the art would have been

7   motivated by the teachings of the prior art regarding the nature of SSL transmissions.

8

9

10   ***Response to Arguments***

11

12   Applicant's arguments filed 4/2/08 have been fully considered but they are not

13   persuasive.

14

15   Essentially, the Applicant argues:

16

17   (i)   *It is asserted that it would have been obvious to one skilled in the art to recognize*

18   *the benefits of acceleration of Gast within the system of Aziz.*

19   *Reasons Why Examiner's Assertion is Incorrect … Here, the applicant points out quite*

20   *clearly that the art cited is deficient in lacking the claimed structure. There are indeed*

21   *claimed differences between the prior art and the claims. At the time of the invention,*

1   *the level of skill in the art has not been shown to have developed as to the art nor as to*

2   *any like claimed structure or disclosure in the cited art.* (Remarks, pg. 18, 20)

3

4   In response, the examiner respectfully notes that the applicant asserts clear

5   differences between the prior art and the claims and that the cited art lacks the claimed

6   structure. However, the applicant fails to provide any support or evidence for the

7   assertion. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they

8   amount to a general allegation that the claims define a patentable invention without

9   specifically pointing out how the language of the claims patentably distinguishes them

10   from the references. Furthermore, regarding the level of one of ordinary skill in the art,

11   the examiner respectfully notes that the prior art itself gives evidence to the level of skill

12   possessed by a practitioner of the art.

13

14   (ii)   *Each prior art paradigm fails to show multiple SSL connections established*

15   *between the same client and server wherein a given certificate and a copy of the*

16   *certificate are employed.*

17   *Aziz only discloses making a single connection between each client and a relay*

18   *and a relay and a server. Aziz states that the connection can be a cleartext HTTP*

19   *connection (non-secure).* (Remarks, pg. 21, 22)

20

21   In response, the examiner respectfully notes that that the prior art shows multiple

22   SSL connections established between the same client and server (e.g. see fig. 3 - one

1   SSL connection (310) and another SSL connection (330) between a client (300) and a

2   server (340); see also 5:34-41).

3

4   (iii)   *There is no disclosure, suggestion or teaching in Aziz as to the need or means*

5   *for making multiple SSL connections with the same client and server. Nor is there any*

6   *disclosure, teaching or suggestion of SSL acceleration server software operably*

7   *associated with a web server computer which ...* (Remarks, pg. 26)

8

9   In response to applicant's arguments against the references individually, one

10 cannot show nonobviousness by attacking references individually where the rejections

11 are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

12 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir.

13 1986).

14

15 (iv)   *Applicants assert Gast teaches away from the instant invention. The Examiner*

16 *asserts that Gast does not a teaching away from the instant invention.*

17   *It is recognized that teaching away requires discouragement of the invention.*

18 *What a reference teaches or suggests must be examined in the context of knowledge,*

19 *skill and reasoning ability of a skilled artisan. Gast recognizes the problem of encryption*

20 *latency, paragraph [0015] of Gast. This latency can be encountered between a client*

21 *server relationship. Gast chooses to offload the cryptographic process to central*

22 *cryptographic hardware component employing an intermediary device to deal with the*

1   *issue as opposed to creating an additional potential encryption latency issue between a*

2   *server and client.* (Remarks, pg. 27)

3

4   In response, the examiner respectfully notes that the applicant provides an

5   asserted characterization of the prior art while failing to give any evidence that the prior

6   art teaches away or from the claimed invention.

7

8   (v)   *The concept presented by the instant invention is in creating multiple SSL direct*

9   *connections between the same client and server is discouraged by the prior art with the*

10 *recognition of such connections causing encryption latency issues. Further, there is no*

11 *teaching of how to create such direct multiple SSL connections between the same client*

12 *and server in a manner to enhance performance and deal with latency issues directly*

13 *between the same client and server employing a given CA certificate and a pseudo*

14 *copy thereof.*

15   *Like Aziz, in Freed et al. there is no direct link between the client computer and*

16 *the server computer.* (Remarks, pg. 27, 28)

17

18   In response to applicant's argument that the references fail to show certain

19 features of applicant's invention, it is noted that the features upon which applicant relies

20 (i.e., *creating multiple SSL direct connections between the same client and server;*

21 *direct multiple SSL connections between the same client and server in a manner to*

22 *enhance performance and deal with latency issues directly between the same client and*

1   *server employing a given CA certificate and a pseudo copy thereof; direct link between*

2   *the client computer and the server computer*) are not recited in the rejected claim(s).

3   Although the claims are interpreted in light of the specification, limitations from the

4   specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26

5   USPQ2d 1057 (Fed. Cir. 1993).

6

7   (vi)   *The instant invention enables secure data be transacted using the CA certificate*

8   *from the web server over an initial SSL connection for transacting key data which must*

9   *pass over such connection, such as when connecting to a secure bank site, for*

10   *example. In addition, the instant invention provides the pseudo CA certificate and*

11   *secondary SSL connection through which data may pass in a secure connection which*

12   *enables functional operations (optimization techniques) to be performed thereon, such*

13   *as compression of data. This is not taught, disclosed or suggested in Freed et al. (or*

14   *Aziz) and this can't be accomplished in the teachings of Freed et al or Aziz. Freed et al.*

15   *only acts as an intermediary intercepting all communication over the existing SSL*

16   *connection and passes the data accordingly, paragraph [0039]. Paragraphs [0052] -*

17   *[0053] and the claims in Freed et al. further illustrate Freed et al. are only concerned*

18   *with providing a classic SSL connection between the client and server through an*

19   *intermediary device.* (Remarks, pg. 29)

20

21   Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount

22   to a general allegation that the claims define a patentable invention without specifically

1   pointing out how the language of the claims patentably distinguishes them from the

2   references.

3   In response to applicant's arguments against the references individually, one

4   cannot show nonobviousness by attacking references individually where the rejections

5   are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

6   USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir.

7   1986).

8

9   ***Conclusion***

10

11   The prior art made of record and not relied upon is considered pertinent to

12   applicant's disclosure:

13   **See Notice of References Cited.**

14

15   A shortened statutory period for reply is set to expire **3** months (not less than 90

16   days) from the mailing date of this communication.

17   Any inquiry concerning this communication or earlier communications from the

18   examiner should be directed to Jeffery Williams whose telephone number is (571) 272-

19   7965. The examiner can normally be reached on 8:30-5:00.

20   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

21   supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

1   number for the organization where this application or proceeding is assigned is (703)

2   872-9306.

3   Information regarding the status of an application may be obtained from the

4   Patent Application Information Retrieval (PAIR) system. Status information for

5   published applications may be obtained from either Private PAIR or Public PAIR.

6   Status information for unpublished applications is available through Private PAIR only.

7   For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

8   you have questions on access to the Private PAIR system, contact the Electronic

9   Business Center (EBC) at 866-217-9197 (toll-free).

10

11
12   J. Williams
13   AU 2137
14
15   /Emmanuel L. Moise/
16   Supervisory Patent Examiner, Art Unit 2137